Available online at www.sciencedirect.com

ScienceDirect

Discrete Mathematics 308 (2008) 2862–2867

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Permutation decoding for binary codes from lattice graphs

J.D. Key[1], P. Seneviratne

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634, USA

Received 28 February 2003; received in revised form 28 June 2004; accepted 21 June 2006
Available online 8 June 2007

Abstract

By finding explicit PD sets, we show that permutation decoding can be used for the binary code obtained from the row span over the field $\mathbb{F}_2$ of an adjacency matrix of the lattice graph $L_2(n)$ for any $n \geqslant 5$.

Keywords: Lattice graph; Permutation decoding

1. Introduction

For any $n \geqslant 2$, the lattice graph $L_2(n)$ is defined to be the line graph of the complete bipartite graph $K_{n,n}$. It is a strongly regular graph on $v = n^2$ vertices, i.e. on the ordered pairs of letters (i, j) where $i, j \in \Omega = \{1, \ldots, n\}$, with valency $2(n-1)$. The binary codes formed from the row span of adjacency matrices of lattice graphs have been examined by Tonchev [13, p. 171] and Haemers et al. [7, Theorem 4.2]. See also [4,5,1,2]. In particular the dimension and weight enumerator of these codes are easily determined. Here, similar to the method in [9] where permutation-decoding sets for the binary codes from the strongly regular triangular graphs were obtained, we obtain explicit permutation-decoding sets for the binary codes from the lattice graphs:

Theorem 1. *For $n \geqslant 5$, let C be the $[n^2, 2(n-1), 2(n-1)]$ binary code from the row span of an adjacency matrix for the lattice graph $L_2(n)$. Then a PD set of n^2 elements can be found for C. Using the $2(n-1)$ points (ordered pairs)*

$$\{(i, n) | 2 \leqslant i \leqslant n-1\} \cup \{(n, i) | 1 \leqslant i \leqslant n\}$$

as information symbols, the set

$$\mathcal{S} = \{((i, n), (j, n)) | 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n\} \tag{1}$$

of permutations in $S_n \times S_n$, in the natural action on the points (ordered pairs), forms a PD set of size n^2 for C.

(*Note*: Here (n, n) denotes the identity element of S_n.)

The proof of this is in Section 4. In Section 2 we give some background material and in Section 3 we obtain results necessary for the theorem.

[1] This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research under Grant N00014-00-1-0565.
E-mail address: keyj@clemson.edu (J.D. Key).

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2006.06.049

2. Background and terminology

Following generally the notation as in [1], an incidence structure $\mathscr{D} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, with point set $\mathscr{P}$, block set $\mathscr{B}$ and incidence $\mathscr{I}$ is a $t-(v, k, \lambda)$ design, if $|\mathscr{P}| = v$, every block $B \in \mathscr{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The design is *symmetric* if it has the same number of points and blocks.

The *code C_F of the design $\mathscr{D}$* over the finite field F is the space spanned by the incidence vectors of the blocks over F. If the point set of $\mathscr{D}$ is denoted by $\mathscr{P}$ and the block set by $\mathscr{B}$, and if $\mathscr{Q}$ is any subset of $\mathscr{P}$, then we will denote the incidence vector of $\mathscr{Q}$ by $v^{\mathscr{Q}}$. Thus $C_F = \langle v^B | B \in \mathscr{B} \rangle$, and is a subspace of $F^{\mathscr{P}}$, the full vector space of functions from $\mathscr{P}$ to F.

The codes here will be *linear codes*, i.e. subspaces of the ambient vector space. If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$, or simply $[n, k, d]$ when $q = 2$, to show this information. A *generator matrix* for the code is a $k \times n$ matrix made up of a basis for C. The *dual* or *orthogonal* code $C^\perp$ is the orthogonal under the standard inner product (,), i.e. $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$. A *check* (or *parity-check*) matrix for C is a generator matrix H for $C^\perp$; the *syndrome* of a vector $y \in F^n$ is Hy^{T}. A code C is *self-orthogonal* if $C \subseteq C^\perp$ and is *self-dual* if $C = C^\perp$. If $c \in C$ then the *support* of c is the set of non-zero coordinate positions of c, and the *weight* of c is the cardinality of the support. A *constant vector* is one for which all the coordinate entries are either 0 or 1. The *all-one vector* will be denoted by $\jmath$, and is the constant vector of weight the length of the code. Two linear codes of the same length and over the same field are *isomorphic* if they can be obtained from one another by permuting the coordinate positions. Any code is isomorphic to a code with generator matrix in so-called *standard form*, i.e. the form $[I_k|A]$; a check matrix then is given by $[-A^{\mathrm{T}}|I_{n-k}]$. The first k coordinates are the *information symbols* and the last $n-k$ coordinates are the *check symbols*. An *automorphism* of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\mathrm{Aut}(C)$. Any automorphism clearly preserves each weight class of C.

Terminology for *graphs* is also standard: the graphs, $\Gamma = (V, E)$ with vertex set V and edge set E, are undirected and the *valency* of a vertex is the number of edges containing the vertex. A graph is *regular* if all the vertices have the same valency; a regular graph is *strongly regular* of type (n, k, λ, μ) if it has n vertices, valency k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices. The *line graph* of a graph $\Gamma = (V, E)$ is the graph $\Gamma^t = (E, V)$ where e and f are adjacent in Γ^t if e and f share a vertex in Γ. The *complete bipartite graph* $K_{n,n}$ on $2n$ vertices with n^2 edges has for line graph the *lattice graph* $L_2(n)$, which has vertex set the set of ordered pairs $\{(i, j) | 1 \leqslant i, j \leqslant n\}$, where two pairs are adjacent if and only if they have a common coordinate. $L_2(n)$ is strongly regular of type $(n^2, 2(n-1), n-2, 2)$.

Permutation decoding was first developed by MacWilliams [10] and involves finding a set of automorphisms of a code called a PD set. The method is described fully in MacWilliams and Sloane [11, Chapter 15] and Huffman [8, Section 8]. A *PD set* for a t-error-correcting code C is a set $\mathscr{S}$ of automorphisms of C which is such that then every possible error vector of weight $s \leqslant t$ can be moved by some member of $\mathscr{S}$ to another vector where the s non-zero entries have been moved out of the information positions. In other words, every t-set of coordinate positions is moved by at least one member of $\mathscr{S}$ to a t-set consisting only of check-position coordinates. That such a set will fully use the error-correction potential of the code follows easily and is proved in Huffman [8, Theorem 8.1]. Such a set might not exist at all, and the property of having a PD set might not be invariant under isomorphism of codes. Furthermore, there is a bound on the minimum size that the set $\mathscr{S}$ may have, due to Gordon [6], from a formula due to Schönheim [12], and quoted and proved in [8]:

Result 1. *If $\mathscr{S}$ is a PD set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n - k$, then*

$$|\mathscr{S}| \geqslant \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

The algorithm for permutation decoding is as follows: we have a t-error-correcting $[n, k, d]_q$ code C with check matrix H in standard form. Thus the generator matrix $G = [I_k|A]$ and $H = [A^{\mathrm{T}}|I_{n-k}]$, for some A, and the first k coordinate positions correspond to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most t errors occur. Let $\mathscr{S} = \{g_1, \ldots, g_s\}$ be the PD set. Compute the syndromes $H(yg_i)^{\mathrm{T}}$

for $i = 1, \ldots, s$ until an i is found such that the weight of this vector is t or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

3. The binary codes

Let $n \geqslant 2$ be any integer and let $L_2(n)$ denote the lattice graph with vertex set $\mathscr{P}$ the n^2 ordered pairs (i, j), $1 \leqslant i, j \leqslant n$. The 1-design $\mathscr{D} = (\mathscr{P}, \mathscr{B})$ will have point set $\mathscr{P}$ and for each point $(i, j) \in \mathscr{P}$, $1 \leqslant i, j \leqslant n$, a block, which we denote by $\overline{(i, j)}$, is defined in the following way:

$$\overline{(i, j)} = \{(i, k) | k \neq j\} \cup \{(k, j) | k \neq i\}.$$

Then the block set is

$$\mathscr{B} = \{\overline{(i, j)} | 1 \leqslant i, j \leqslant n\}.$$

The incidence vector of the block $\overline{(i, j)}$ is

$$v^{\overline{(i,j)}} = \sum_{k \neq j} v^{(i,k)} + \sum_{k \neq i} v^{(k,j)} = \sum_{k=1}^{n} v^{(i,k)} + \sum_{k=1}^{n} v^{(k,j)}, \tag{2}$$

where, as usual with the notation from [1], the incidence vector of the subset $X \subseteq \mathscr{P}$ is denoted by v^X, but writing $v^{(i,j)}$ instead of $v^{\{(i,j)\}}$. To avoid trivial cases we will take $n \geqslant 5$.

First we summarize the known properties of $L_2(n)$, its automorphism group, and its binary code, that we will be needing. The proofs can be found in [7,13].

Result 2. *For $n \geqslant 5$, the automorphism group of the lattice graph $L_2(n)$ is $S_n \wr S_2$, the wreath product of S_n with S_2. The binary code formed by the row space over $\mathbb{F}_2$ of an adjacency matrix for $L_2(n)$ is a $[n^2, 2(n-1), 2(n-1)]$ code with $S_n \wr S_2$ acting as an automorphism group.*

The lattice graph $L_2(n)$ can be considered as a rank-3 graph defined by the action of the group $G = S_n \wr S_2$. This group is constructed as an extension of the group $H = S_n \times S_n$ by $S_2 = \{1, \tau\}$, where $\tau^2 = 1$. The element τ acts on H via $(\alpha, \beta)^\tau = (\beta, \alpha)$, for $\alpha, \beta \in S_n$. Further, G acts as a rank-3 group on $\mathscr{P} = \Omega \times \Omega$, where $\Omega = \{1, 2, \ldots, n\}$, in the following way:

$$(i, j)^{(\alpha,\beta)} = (i^\alpha, j^\beta) \quad \text{and} \quad (i, j)^\tau = (j, i), \tag{3}$$

where $(i, j) \in \mathscr{P}$, $(\alpha, \beta) \in H$, $\tau = (1, 2) \in S_2$.

In all the following lemmas $C = \langle v^{\overline{(i,j)}} | (i, j) \in \mathscr{P} \rangle$ will denote the binary code of the design $\mathscr{D}$ (equivalently of the graph $L_2(n)$), and $C^\perp$ will be its dual code.

Lemma 1. *For every $\sigma \in S_n$, the vector*

$$w(\sigma) = \sum_{i=1}^{n} v^{(i,i\sigma)} \tag{4}$$

is in $C^\perp$.

Proof. Let $v^{\overline{(i,j)}} \in C$ and $\sigma \in S_n$. Then

$$\begin{aligned}(w(\sigma), v^{\overline{(i,j)}}) &= \left(\sum_{m=1}^{n} v^{(m,m\sigma)}, \sum_{k \neq j} v^{(i,k)} + \sum_{k \neq i} v^{(k,j)} \right) \\ &= \left(v^{(i,i\sigma)}, \sum_{k \neq j} v^{(i,k)} \right) + \left(v^{(j\sigma^{-1},j)}, \sum_{k \neq i} v^{(k,j)} \right).\end{aligned}$$

Now $(v^{(i,i\sigma)}, \sum_{k\neq j} v^{(i,k)}) = 0$ if $i\sigma = j$, i.e. if $j\sigma^{-1} = i$, which implies that $(v^{(j\sigma^{-1},j)}, \sum_{k\neq i} v^{(k,j)}) = 0$. Conversely, $(v^{(i,i\sigma)}, \sum_{k\neq j} v^{(i,k)})=1$ if $i\sigma \neq j$, i.e. if $j\sigma^{-1} \neq i$, which implies that $(v^{(j\sigma^{-1},j)}, \sum_{k\neq i} v^{(k,j)})=1$. Thus $(w(\sigma), v^{\overline{(i,j)}})= 0$, as required. □

Lemma 2. *The minimum weight of $C^{\perp}$ for $n \geqslant 5$ is* 4.

Proof. For any $\sigma \in S_n$, $w(\sigma) \in C^{\perp}$ by Lemma 1. For any $i, j \in \Omega$, where $i \neq j$, write

$$w(i, j; \sigma) = w(\sigma) + w((i, j)\sigma) = v^{(i,i\sigma)} + v^{(i,j\sigma)} + v^{(j,i\sigma)} + v^{(j,j\sigma)}, \tag{5}$$

where here (i, j) denotes the transposition $(i, j) \in S_n$, so that $C^{\perp}$ has words of weight 4.

To show that $C^{\perp}$ cannot have words of weight less than 4, note first that it cannot have words of weight 1, so suppose it has a word $w = v^{(i,j)} + v^{(k,l)}$ of weight 2. Noting that we can use the automorphism τ (see Eq. (3)) to interchange the members of the ordered pairs in the points, we find that there are seven distinct cases to consider for the two points (i, j) and (k, l) and in each case we find a block of the design that meets one of the points but not the other, thus having inner product 1 with w. This shows that $C^{\perp}$ cannot have words of weight 2. Now suppose there is a word $w = v^{(i,j)} + v^{(k,l)} + v^{(m,p)}$ of weight 3. Consideration of the various types of triples of points, along with the use of the automorphism τ, leads again easily to the existence, in each case, of a block of the design that meets w in only one point. There are a few more cases to deal with than the weight-2 case, but again we omit the details. Thus the minimum weight of $C^{\perp}$ is 4. □

In the special case where $\sigma = (i, k)(j, l)$, where $k, l \in \Omega$, $k \neq l$, using the notation of (5), we write

$$u(\{i, j\}; \{k, l\}) = w(i, j; (i, k)(j, l)) = v^{(i,k)} + v^{(i,l)} + v^{(j,k)} + v^{(j,l)}, \tag{6}$$

for this weight-4 word of $C^{\perp}$, since the ordering of i and j or of k and l is arbitrary.

Lemma 3. *A sequence $\mathcal{U}$ of weight-4 vectors $u(i, j; k, l)$ can be found such that $\mathcal{U}$ together with $\jmath$ forms a basis for $C^{\perp}$ when n is odd, and $\mathcal{U}$ together with $w(\sigma)$ where $\sigma = (1, 2, \ldots, n)$ forms a basis when n is even.*

Proof. Note that $w(\sigma)$ is defined in Eq. (4). We first describe the sequence $\mathcal{U}$, and take a specific ordering of the points $\mathcal{P}$ so that we get a matrix of the vectors in $\mathcal{U}$ in upper triangular form. Thus let S be a sequence $\{s_i\}_{i=1}^{n-1}$ of length $n - 1$ of pairs $s_1 = \{1, 2\}$, $s_2 = \{2, 3\}$, and so on, with $s_i = \{i, i + 1\}$, and $s_{n-1} = \{n - 1, n\}$. Then we define $\mathcal{U}$ as follows: first take $u(s_1; s_1), u(s_1; s_2), \ldots, u(s_1; s_{n-1})$, followed by $u(s_2; s_1), u(s_2; s_2), \ldots, u(s_2; s_{n-1})$, and so on, until $u(s_{n-1}; s_1), \ldots, u(s_{n-1}; s_{n-1})$. This gives $(n - 1)^2$ vectors, and if the points are ordered as we will now describe, it will be seen that we have an upper triangular matrix of rank $(n - 1)^2$.

The point ordering is as follows: first we take, in order,

$$\mathcal{P}_1 = \{(1, 1), (1, 2), \ldots, (1, n - 1), (2, 1), (2, 2), \ldots, (n - 1, 1), \ldots, (n - 1, n - 1)\} \tag{7}$$

giving $(n - 1)^2$ points, followed by

$$\mathcal{P}_2 = \{(1, n), (2, n), \ldots, (n - 1, n), (n, 1), (n, 2), \ldots, (n, n)\}, \tag{8}$$

for the remaining $2n - 1$ points. Since the dimension of $C^{\perp}$ is $(n - 1)^2 + 1$, we need a further element and we will show that the first point, $(1, n)$, of $\mathcal{P}_2$ of Eq. (8) can be included in the information set for $C^{\perp}$. The proofs for the odd and even cases are distinct. First some notation: let

$$U(i; k) = u(\{i, i + 1\}; \{k, k + 1\}) = v^{(i,k)} + v^{(i,k+1)} + v^{(i+1,k)} + v^{(i+1,k+1)}. \tag{9}$$

For n odd, let

$$w = \sum_{i=0}^{(n-3)/2} \sum_{j=0}^{(n-3)/2} U(2i + 1; 2j + 1).$$

Then $w \in \langle \mathscr{U} \rangle$, and it is quite direct to verify that $w = \sum_{1 \leqslant i,j \leqslant n-1} v^{(i,j)}$ and that $w + \jmath = \sum_{n \in \{i,j\}} v^{(i,j)}$. Thus if $\jmath$ is added at the bottom of the matrix, we can reduce the matrix to upper triangular form with the shown selection of elements of $\mathscr{U}$, thereby increasing the rank by 1. We can include the point $(1, n)$ in the information symbols for $C^\perp$ since it has coordinate 1 in $w + \jmath$. (Note of course that $\jmath \in C^\perp$ since C is spanned by vectors of even length.)

For n even, let $B_i = \{2, 4, \ldots, 2i\}$, for $i = 1, 2, \ldots, n/2$. Then if $w = w_1 + w_2 + w_3 + w_4$ where

$$
\begin{aligned}
w_1 &= \sum_{i=2}^{n-1} U(1; i), \\
w_2 &= \sum_{l=1}^{n/2-2} \sum_{i \in B_l} (U(2l+1; i) + U(2l; i)), \\
w_3 &= \sum_{l=1}^{n/2-2} \sum_{i=2l+2}^{n-1} U(2l+1; i), \\
w_4 &= \sum_{i \in B_{n/2-1}} (U(n-2; i) + U(n-1; i)),
\end{aligned}
$$

we have $w \in \langle \mathscr{U} \rangle$, and it is quite direct to verify that

$$
\begin{aligned}
w_1 &= v^{(1,2)} + v^{(2,2)} + v^{(1,n)} + v^{(2,n)}, \\
w_2 &= \sum_{i=1}^{n/2-2} v^{(2i,2i)} + \sum_{i=1}^{n/2-2} v^{(2i,2i+1)} + \sum_{i=2}^{n-3} v^{(n-2,i)}, \\
w_3 &= \sum_{i=3}^{n-2} v^{(i,n)} + \sum_{i=1}^{n/2-2} v^{(2i+1,2i+2)} + \sum_{i=2}^{n/2-1} v^{(2i,2i)}, \\
w_4 &= \sum_{i=2}^{n-1} v^{(n,i)} + \sum_{i=2}^{n-1} v^{(n-2,i)},
\end{aligned}
$$

and thus, with $\sigma = (1, 2, \ldots, n) \in S_n$,

$$
w = w(\sigma) + \sum_{i=1}^{n-1} (v^{(i,n)} + v^{(n,i)}),
$$

since $w(\sigma) = \sum_{i=1}^{n} v^{(i,i\sigma)} = v^{(1,2)} + v^{(2,3)} + \cdots + v^{(n-1,n)} + v^{(n,1)}$. Thus adjoining $w(\sigma)$ to $\mathscr{U}$ will produce an upper triangular matrix of rank $(n-1)^2 + 1$, as in the odd case, and the point $(1, n)$ can be placed in the information positions. This completes the proof. □

4. PD sets

We can now prove Theorem 1. We showed in Lemma 3 that the point ordering given in Eqs. (7) and (8) gave the generator matrix for $C^\perp$ in standard form. Thus we may take the $2(n-1)$ points from Eq. (8), starting with $(2, n)$, as our information symbols for C.

Proof of theorem. Denote the information symbols by $\mathscr{I}$. Now C can correct $t = n - 2$ errors, so we need to show that every set of $s \leqslant t$ points can be moved by some element of $\mathscr{S}$ into the check positions $\mathscr{E}$. Let

$$
\mathscr{T} = \{(a_1, b_1), (a_2, b_2), \ldots, (a_s, b_s)\}
$$

be a set of $s \leqslant t = n - 2$ points of $\mathscr{P}$. If $\Omega_1 = \{a_1, a_2, \ldots, a_s\}$ and $\Omega_2 = \{b_1, b_2, \ldots, b_s\}$, then $|\Omega_i| \leqslant n - 2$ for $i = 1, 2$ and thus we can find $k \neq n$ and $l \neq n$ such that $k \notin \Omega_1$ and $l \notin \Omega_2$. Then $g = ((k, n), (l, n)) \in S_n \times S_n$ will satisfy $\mathscr{T}^g \subseteq \mathscr{E}$. Thus $\mathscr{S}$ forms a PD set for the code. □

Note: The number of elements we have in our PD set for C is n^2; we computed the Gordon bound (see Result 1) using Magma [3] and found that the following formulae for the Gordon bound appear to hold, showing that the bound is linear in n:

- for n odd:

$$n \equiv 9 \pmod{12}, n \geqslant 21: \frac{1}{2}(5n-11) - 2\left\lfloor \frac{n-3}{4} \right\rfloor - \left\lceil \frac{n-5}{6} \right\rceil = \frac{1}{6}(11n-15);$$

$$n \not\equiv 9 \pmod{12}, n \geqslant 29: \frac{1}{2}(5n-11) - 2\left\lfloor \frac{n-3}{4} \right\rfloor - \left\lfloor \frac{n-5}{6} \right\rfloor;$$

- for $n \geqslant 12$ even:

$$2n - 3 - \left\lceil \frac{n-2}{4} \right\rceil + \left\lfloor \frac{n-6}{12} \right\rfloor.$$

Some computations using Magma to find PD sets for a few small values of n yielded sets of size less than n^2, but not as small as the Gordon bound.

References

[1] E.F. Assmus Jr., J.D. Key, Designs and their Codes, in: Cambridge Tracts in Mathematics, vol. 103, Cambridge University Press, Cambridge, 1992 (second printing with corrections, 1993).

[2] E.F. Assmus Jr., J.D. Key, Designs and codes: an update, Des. Codes Cryptogr. 9 (1996) 7–27.

[3] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, November 1994. ⟨http://www.maths.usyd.edu.au:8000/u/magma/⟩.

[4] A.E. Brouwer, C.J. van Eijl, On the p-rank of the adjacency matrices of strongly regular graphs, J. Algebraic Combin. 1 (1992) 329–346.

[5] A.E. Brouwer, J.H. van Lint, Strongly regular graphs and partial geometries, in: D.M. Jackson, S.A. Vanstone (Eds.), Enumeration and Design, Proceedings of the Silver Jubilee Conference on Combinatorics, Waterloo, 1982, Academic Press, Toronto, 1984, pp. 85–122.

[6] D.M. Gordon, Minimal permutation sets for decoding the binary Golay codes, IEEE Trans. Inform. Theory 28 (1982) 541–543.

[7] W.H. Haemers, René Peeters, Jeroen M. van Rijckevorsel, Binary codes of strongly regular graphs, Des. Codes Cryptogr. 17 (1999) 187–209.

[8] W.C. Huffman, Codes and groups, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. 2, Elsevier, Amsterdam, 1998, pp. 1345–1440, (Part 2, Chapter 17).

[9] J.D. Key, J. Moori, B.G. Rodrigues, Permutation decoding for binary codes from triangular graphs, European J. Combin. 25 (2004) 113–123.

[10] F.J. MacWilliams, Permutation decoding of systematic codes, Bell System Tech. J. 43 (1964) 485–505.

[11] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1983.

[12] J. Schönheim, On coverings, Pacific J. Math. 14 (1964) 1405–1411.

[13] Vladimir D. Tonchev, Combinatorial configurations, designs, codes, graphs, in: Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 40, Longman, New York, 1988 (translated from the Bulgarian by Robert A. Melter).